# First-grade The SecOps Group Test CNSP Dumps Demo and Realistic Exam Dumps CNSP Free


P.S. Free 2025 The SecOps Group CNSP dumps are available on Google Drive shared by Real4test: https://drive.google.com/open?id=1b68KC7AUmFjfp8YLemgdLpvTaL2pchiG

After buying the The SecOps Group CNSP practice material, Real4test offers a full refund guarantee in case of unsatisfactory The SecOps Group CNSP test results which are highly unlikely. We also offer a free demo version of the The SecOps Group CNSP exam prep material.

No matter how much you study, it can be difficult to feel confident going into the Certified Network Security Practitioner (CNSP) exam. However, there are a few things you can do to help ease your anxiety and boost your chances of success. First, make sure you prepare with real The SecOps Group CNSP Exam Dumps. If there are any concepts you're unsure of, take the time to take CNSP Practice Exams until you feel comfortable. Buy Certified Network Security Practitioner (CNSP) preparation material from a trusted company such as Real4test. This will ensure you get updated Certified Network Security Practitioner (CNSP) study material to cover everything before the big day.

**>> Test CNSP Dumps Demo <<**

## Pass Guaranteed The SecOps Group - CNSP - Test Certified Network Security Practitioner Dumps Demo

Someone around you must be using our CNSP exam questions. The users of our CNSP exam materials are really very extensive. Or, you can consult someone who has participated in the CNSP exam. They must know or use our products. We can confidently say that our products are leading in the products of the same industry. The richness and authority of CNSP Exam Materials are officially certified.

## The SecOps Group CNSP Exam Syllabus Topics:

| Topic | Details |
|---|---|
| | |

| | |
|---|---|
| Topic 1 | • Common vulnerabilities affecting Windows Services: This section of the exam measures the skills of Network Engineers and focuses on frequently encountered weaknesses in core Windows components. It underscores the need to patch, configure, and monitor services to prevent privilege escalation and unauthorized use. |
| Topic 2 | • TCP<br>• IP (Protocols and Networking Basics): This section of the exam measures the skills of Security Analysts and covers the fundamental principles of TCP<br>• IP, explaining how data moves through different layers of the network. It emphasizes the roles of protocols in enabling communication between devices and sets the foundation for understanding more advanced topics. |
| Topic 3 | • Active Directory Security Basics: This section of the exam measures the skills of Network Engineers and introduces the fundamental concepts of directory services, highlighting potential security risks and the measures needed to protect identity and access management systems in a Windows environment. |
| Topic 4 | • Linux and Windows Security Basics: This section of the exam measures skills of Security Analysts and compares foundational security practices across these two operating systems. It addresses file permissions, user account controls, and basic hardening techniques to reduce the attack surface. |
| Topic 5 | • TLS Security Basics: This section of the exam measures the skills of Security Analysts and outlines the process of securing network communication through encryption. It highlights how TLS ensures data integrity and confidentiality, emphasizing certificate management and secure configurations. |
| Topic 6 | • Open-Source Intelligence Gathering (OSINT): This section of the exam measures the skills of Security Analysts and discusses methods for collecting publicly available information on targets. It stresses the legal and ethical aspects of OSINT and its role in developing a thorough understanding of potential threats. |
| Topic 7 | • Network Scanning & Fingerprinting: This section of the exam measures the skills of Security Analysts and covers techniques for probing and analyzing network hosts to gather details about open ports, operating systems, and potential vulnerabilities. It emphasizes ethical and legal considerations when performing scans. |
| Topic 8 | • This section of the exam measures the skills of Network Engineers and explains how to verify the security and performance of various services running on a network. It focuses on identifying weaknesses in configurations and protocols that could lead to unauthorized access or data leaks. |
| Topic 9 | • This section of the exam measures skills of Network Engineers and explores the utility of widely used software for scanning, monitoring, and troubleshooting networks. It clarifies how these tools help in detecting intrusions and verifying security configurations. |
| Topic 10 | • Social Engineering attacks: This section of the exam measures the skills of Security Analysts and addresses the human element of security breaches. It describes common tactics used to manipulate users, emphasizes awareness training, and highlights how social engineering can bypass technical safeguards. |
| Topic 11 | • Password Storage: This section of the exam measures the skills of Network Engineers and addresses safe handling of user credentials. It explains how hashing, salting, and secure storage methods can mitigate risks associated with password disclosure or theft. |

## The SecOps Group Certified Network Security Practitioner Sample Questions (Q14-Q19):

**NEW QUESTION # 14**
Which of the following is a valid DNS record type?

- A. All of the above
- B. TXT record

- C. SRV record
- D. NAPTR record

**Answer: A**

Explanation:
DNS (Domain Name System) records define how domain names are mapped to various types of data, each serving a specific purpose in network operations. The question asks for valid DNS record types, and all listed options are recognized.
Why D is correct:
A . NAPTR record: The Naming Authority Pointer (NAPTR) record is used for service discovery and mapping domain names to services, protocols, and ports (e.g., in SIP or ENUM systems).
B . SRV record: The Service (SRV) record specifies the hostname and port for specific services (e.g., LDAP, XMPP), aiding in service location.
C . TXT record: The Text (TXT) record stores arbitrary text data, often for SPF, DKIM, or domain verification.
All are valid DNS record types per RFC standards and CNSP documentation, making "All of the above" the correct answer.
Why other options are incomplete: A, B, or C alone exclude other valid types listed, so D is the most comprehensive response.

**NEW QUESTION # 15**
What is the response from a closed TCP port which is not behind a firewall?

- A. A SYN and an ACK packet
- B. ICMP message showing Port Unreachable
- C. A RST and an ACK packet
- D. A FIN and an ACK packet

**Answer: C**

Explanation:
TCP uses a structured handshake, and its response to a connection attempt on a closed port follows a specific protocol when unobstructed by a firewall.
Why C is correct: A closed TCP port responds with a RST (Reset) and ACK (Acknowledgment) packet to terminate the connection attempt immediately. CNSP highlights this as a key scanning indicator.
Why other options are incorrect:
A: ICMP Port Unreachable is for UDP, not TCP.
B: FIN/ACK is for closing active connections, not rejecting new ones.
D: SYN/ACK indicates an open port during the TCP handshake.

**NEW QUESTION # 16**
You are performing a security audit on a company's network infrastructure and have discovered the SNMP community string set to the default value of "public" on several devices. What security risks could this pose, and how might you exploit it?

- A. The potential risk is that an attacker could use the SNMP protocol to modify the devices' configuration settings. You might use a tool like Snmpset to change the settings.
- B. None of the above.
- C. The potential risk is that an attacker could use the SNMP protocol to gather sensitive information about the devices. You might use a tool like Snmpwalk to query the devices for information.
- D. Both A and B.

**Answer: C**

Explanation:
SNMP (Simple Network Management Protocol) uses community strings as a basic form of authentication. The default read-only community string "public" is widely known, and if left unchanged, it exposes devices to unauthorized access. The primary risk with "public" is information disclosure, as it typically grants read-only access, allowing attackers to gather sensitive data (e.g., device configurations, network topology) without altering settings.
Why A is correct: With the "public" string, an attacker can use tools like snmpwalk to enumerate device details (e.g., system uptime, interfaces, or software versions) via SNMP queries. This aligns with CNSP's focus on reconnaissance risks during security audits, emphasizing the danger of default credentials enabling passive data collection.
Why other options are incorrect:

B: While modifying settings is a risk with SNMP, the default "public" string is typically read-only. Changing configurations requires a read-write community string (e.g., "private"), which isn't implied here. Thus, snmpset would not work with "public" alone.
C: Since B is incorrect in this context, C (both A and B) cannot be the answer.
D: The risk in A is valid, so "none of the above" is incorrect.

**NEW QUESTION # 17**
The Active Directory database file stores the data and schema information for the Active Directory database on domain controllers in Microsoft Windows operating systems. Which of the following file is the Active Directory database file?

- A. MSAD.MDB
- B. NTDS.MDB
- C. NTDS.DAT
- D. NTDS.DIT

**Answer: D**

Explanation:
The Active Directory (AD) database on Windows domain controllers contains critical directory information, stored in a specific file format.
Why D is correct: The NTDS.DIT file (NT Directory Services Directory Information Tree) is the Active Directory database file, located in C:\Windows\NTDS\ on domain controllers. It stores all AD objects (users, groups, computers) and schema data in a hierarchical structure. CNSP identifies NTDS.DIT as the key file for AD data extraction in security audits.
Why other options are incorrect:
A . NTDS.DAT: Not a valid AD database file; may be a confusion with other system files.
B . NTDS.MDB: Refers to an older Microsoft Access database format, not used for AD.
C . MSAD.MDB: Not a recognized file for AD; likely a misnomer.

**NEW QUESTION # 18**
How many usable TCP/UDP ports are there?

- A. 0
- B. 1
- C. 2
- D. 3

**Answer: B**

Explanation:
TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) port numbers are defined by a 16-bit field in their packet headers, as specified in RFC 793 (TCP) and RFC 768 (UDP). A 16-bit integer ranges from 0 to 65,535, yielding a total of 65,536 possible ports (2